Infineon Technologies AG Trusted Platform Module SLB9665_2.0 v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00

Description:

The TOE is an integrated circuit and software platform that provides computer manufacturers with the core components of a subsystem used to assure authenticity, integrity and confidentiality in e-commerce and internet communications within a Trusted Computing Platform. The SLB9665_2.0 is a complete solution implementing the version 2.0 of the TCG Trusted Platform Module Library Family “2.0” Specification and the TCG PC Client Specific Platform TPM Profile (PTP) Family “2.0” Specification. The SLB9665_2.0 uses the Low Pin Count Interface (LPC) as defined by Intel for the integration into existing PC mainboards. The SLB9665_2.0 is basically a secure controller with the following added functionalities:

- Random number generator (DRBG)
- Asymmetric key generation (RSA keys with key length up to 2048 bit, EC keys with key length of 256 bits)
- Symmetric key generation (AES keys)
- Symmetric and asymmetric key procedures (encryption/decryption, generation and verification of digital signatures),
- Hash algorithms (SHA-1, SHA-256) and MAC (HMAC)
- Secure key and data storage
- Identification and Authorization mechanisms

Security Assumptions:

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. Security objectives which are relevant for the TOE are:

- The TOE environment is highly variable. In general, the TOE is assumed to be in an uncontrolled environment with no guarantee of the TOE’s physical security.
- The developer of the host platform must ensure that trusted processes indicate their correct locality to the TPM and untrusted processes are able to assert just the locality 0 or Legacy only to the TPM.
- The TOE must be installed and configured properly for starting up the TOE in a secure state. The security attributes of subjects and objects shall be managed securely by the authorised user
- The IT environment must create EK and AK credentials by trustworthy procedures for the root of trust for reporting.
- The platform part of the root of trust for measurement provides a representation of embedded data or program code (measured values) to the TPM for measurement.
- The TCG subsystem, in which the TPM is used, is a trusted subsystem that is an integral part of a computing platform that consists of logical components including the TPM, a connection module and a control software e.g. the TCG Software Stack.
- In general the TPM provides cryptographic capabilities and protected storage.

Attacker threats:
This section shows the threats that are to be countered by the TOE, its development environment, its operational environment, or a combination of these three:

- An undetected compromise of the data in shielded locations may occur as a result of an attacker (whether an insider or outsider) attempting to perform actions that the individual or capability is not authorised to perform
- An unauthorised individual or user may tamper with TSF, security attributes or other data in order to bypass TOE security functions and gain unauthorised access to TOE assets.
- A user or an attacker may export data from shielded locations without security attributes or with insecure security attributes, causing the data exported to be erroneous and unusable, to allow erroneous data to be added or substituted for the original data, and/or to reveal secrets.
- Cryptographic key generation or operation may be incorrectly implemented, allowing an unauthorised individual or user to compromise keys generated within the TPM or encrypted data or to modify data undetected.
- An unauthorised individual or user of the TOE may cause unauthorised disclosure or modification of TOE assets by physically interacting with the TOE. The attacker may be a hostile user of the TOE.
- An unauthorised individual may impersonate an authorised user of the TOE (e.g. by dictionary attacks to guess the authorisation data) and thereby gain access to TOE data in shielded locations and protected capabilities.
- A user or attacker may import data without security attributes or with erroneous security attributes, causing key ownership and authorisation to be uncertain or erroneous and the system to malfunction or operate in an insecure manner.
- The TOE may start-up in an insecure state or enter an insecure state, allowing an attacker to obtain sensitive data or compromise the system.
- An attacker may intercept the communication between a user and the TPM subjects to gain knowledge of the commands and data sent to the subject or manipulate the communication.
- TOE assets may be modified or disclosed to an unauthorised individual or user of the TOE, through malfunction of the TOE.
- An attacker may modify data in shielded locations or their security attributes in order to gain access to the TOE and its assets.
- A user or attacker may create an object with no security attributes or make unauthorised changes to security attribute values for an object to enable attacks.
- An unauthorised individual may gain access to the system and sensitive data through a “replay” or “man-in-the-middle” attack that allows the individual to capture identification and authentication data.
- An originator of data may deny originating the data to avoid accountability.
- A user may obtain information that the user is not authorised to have when the data in shielded locations is no longer actively managed by the TOE (“data scavenging”).
- An attacker may exploit information which is leaked from the TOE during usage of the TSF in order to disclose confidential assets.

Security assurance requirements:

This Protection Profile claims to be conformant with the Common Criteria version 3.1 Release 4 as follows - Part 2 extended, - Part 3 conformant.

The Security Assurance Requirements (SAR) for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) as defined in CC part 3 and augmented with ALC_FLR.1 and AVA_VAN.4.

#	Assurance Class	Assurance Component	Assurance Components description
1	ADV: Development	ADV_ARC.1	Security architecture description
2		ADV_FSP.4	Complete functional specification
3		ADV_IMP.1	Implementation representation of the TSF
4		ADV_TDS.3	Basic modular design
5	AGD: Guidance documents	AGD_OPE.1	Operational user guidance
6		AGD_PRE.1	Preparative procedures
7	ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
8		ALC_CMS.4	Problem tracking CM coverage
9		ALC_DEL.1	Delivery procedures
10		ALC_DVS.1	Identification of security measures
11		ALC_LCD.1	Developer defined life-cycle model
12		ALC_FLR.1	Basic flow remediation -- augmented
13		ALC_TAT.1	Well-defined development tools
14	ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
15		ASE_ECD.1	Extended components definition
16		ASE_INT.1	ST introduction
17		ASE_OBJ.2	Security objectives
18		ASE_REQ.2	Derived security requirements
19		ASE_SPD.1	Security problem definition
20		ASE_TSS.1	TOE summary specification

21	ATE: Tests	ATE_COV.2	Analysis of coverage
22		ATE_DPT.1	Testing: basic design
23		ATE_FUN.1	Functional testing
24		ATE_IND.2	Independent testing – sample
25	AVA : Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis -- augmented

Security Functional Components:

The security functional requirements for the TOE are defined and described here: https://www.commoncriteriaportal.org/files/ppfiles/TCG_PP_PC_client_specific_TPM_SecV2_v10.pdf
section 7.1 Security Functional Requirements
They defines the subjects, objects and operations and introduces the notation for the operation of the SFR components. In summary:

Cryptographic Support:
Generation of random numbers, generation of asymmetric key pairs, RSA and ECC digital signature (generation and verification), RSA, ECC and AES data encryption and decryption, key destruction, the generation of hash values and the generation and verification of MAC values.

Identification and Authentication:
Mechanisms for the identification and authentication capability to authorize the use of an Protected Object and Protected Capability using authentication values or policies.

General and Test:
Provision and enforcement of the TPM role model, startup- and self tests, preservation of secure state in case of failures or shutdown, and resistance to physical manipulation or probing.

Object Hierarchy:
State control on all subjects, objects and operations, modification of security attributes, provision of TPM hierarchy model, monitoring of data storage, enforcement of object hierarchy.

TOE Operation:
Access control on different subjects, objects and operations, enforcement of different rules of operation and interaction between subjects and objects, enabling and disabling of functions, enforcement of NVM restrictions, and creation of evidence of origin.

Testing and evaluation:
The tests were performed by the developers and evaluators.
The evaluation was completed on 18 April 2018. TÜV Informationstechnik GmbH is an evaluation facility recognised by the certification body of BSI (Federal Office for Information Security)

The development tests are divided into 6 categories:

- Simulation Tests (design verification)
- Qualification Tests
- Verification Tests
- Security Evaluation Tests
- Production Tests
- Software Tests

They cover all security functionalities and all security mechanisms as identified in the functional specification.

The evaluators were able to repeat the tests of the developer, either using the tools and TOE samples delivered to the evaluator, or at the developer's site.

The evaluation has shown that the actual version of the TOE provides the security functionalities as specified by the developer. The test results confirm the correct implementation of the TOE security functionalities.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure

Penetration Testing:
The penetration testing was partially performed using the developer's testing environment, partially using the test environment of the evaluation body.
All configurations of the TOE being intended to be covered by the current evaluation were tested.
The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Moderate was actually successful.

Attack scenarios having been tested:

- Statistical tests of the TOE DRNG
- Find undocumented capabilities which are sent by the TOE as response to TPM2_GetCapabilitiy command.
- Try to circumvent access control by injecting faults through laser light (LFI attack).
- Effectiveness of the TOE security functionality.
- Effectiveness of filters and detectors.
- Effectiveness of bus and memory encryption.
- Differential Fault Analysis.
- Simple and Differential Power Analysis.

- EMA / SEMA / DEMA Attacks.
- Effectiveness of deactivation of test functions.
- Bypass of dictionary attack counter.
- Intentional misuse of TPM commands.
- Brute force of authValues. (AuthValues are for entity that use objects keys, data in NV memory)
- Tearing on LPC communication interface.

SFRs penetration tested:
The following TSF interfaces have been tested:

- Electrical interface
- Data Interface
- SF_CRY (Cryptographic Support)
- SF_I&A (Identification and Authentication)
- SF_G&T (General and Test)
- SF_OBH (Object Hierarchy)
- SF_TOP (TOE Operation)

All security features of the TOE have been addressed by penetration testing.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure.

Conclusion:

The TOE is covers a large amount of security needs in just one package. It is rigorously tested and even has guidelines on its identification and shipping. This product is widely by a lot of organisations and manufacturers, therefore is also prone to more attacks.